

## UNITED STATES DISTRICT COURT

for the  
District of Oregon

FILED 9 JAN '19 15:46 USDC-ORP

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)The property located at 11412 SE Quail Run Drive,  
Happy Valley, Oregon 97086 as described in Attachment  
A

Case No. '19 -MC- 13

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The property located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086 as described in Attachment A hereto,

located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 1349

18 U.S.C. § 1343

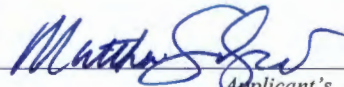
Offense Description

Conspiracy To Commit Wire Fraud

Wire Fraud

The application is based on these facts:  
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



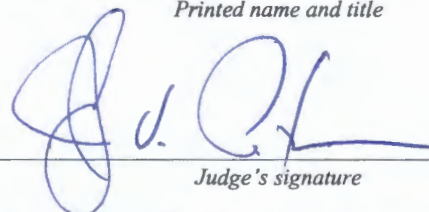
Applicant's signature

MATTHEW SWANSINGER, SPECIAL AGENT, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 1.9.19



Judge's signature

City and state: PORTLAND, Oregon

HON. JOHN V. ACOSTA, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF MATT SWANSINGER

**Affidavit in Support of an Application  
Under Rule 41 for a Search Warrant**

I, Matt Swansinger, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since March of 2008. I am currently assigned to the Portland Division of the FBI, White Collar Crime Squad. In this capacity, I am charged with investigating violations of federal criminal law, specifically those involved with complex financial crimes. I perform and have performed a variety of investigative tasks, including functioning as a case agent on corporate fraud cases, identity theft cases, fraud against the government, public corruption, and virtual currency fraud cases. I have received training in the conduct of computer crime investigations. I also have received training and gained experience in interviewing and interrogation techniques, and the execution of federal search warrants and seizures.

2. This affidavit is submitted in support of an Application for a Search and Seizure Warrant on the residence belonging to Ronnie Stevens, also known as Tim Ephrem, Tim J. Ephrem, Ron Steves, Ron Stevens, Ron Stephens, and Tina Ephrem, also known as Lisa Peterson.

3. This Application for Search and Seizure Warrant is for evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code § 1349, Conspiracy and Title 18, United States Code § 1343, Wire Fraud. As set forth, below, I have probable cause to believe that such items, as set forth in Attachment B, which is attached hereto and incorporated

herein by this reference, are currently on the premises located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086, and is more fully described in Attachment A, which is attached hereto and incorporated herein by this reference.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

#### **Applicable Law**

5. Title 18 United States Code § 1349, Conspiracy states that: Any person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

6. Title 18 United States Code § 1343, Fraud by wire, radio, or television (Wire Fraud) states in part that: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years or both.

7. Based upon the facts set forth in this affidavit, I believe there is probable cause that Ronnie Stevens (hereinafter referred to as Stevens), also known as Tim Ephrem, and/or Ron Stevens, date of birth July 11, 1969, and social security number 535-78-3850, and Tina Ephrem date of birth May 25, 1975, and social security number 540-15-3767 both conspired to defraud victims in order to obtain money in violation of Title 18, United States Code, § 1343, wire fraud.

#### **Statement of Probable Cause**

8. For the reasons detailed below, there is probable cause to believe, and I do believe, that Stevens and Tina Ephrem conspired to create, establish, manage, and to defraud victims in a conspiracy to commit wire fraud in order to obtain money in violation of Title 18, United States Code, § 1349, Conspiracy, and Title 18, United States Code §1343, wire fraud (hereinafter referred to as the Target Offenses). Further, there is probable cause to believe, and I do believe, that evidence, instrumentalities, contraband, and fruits of the Target Offenses are currently on the premises located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086.

#### **Initiation of Investigation**

9. On or about May 31, 2018, the FBI met with representatives from the United States Attorney's Office (USAO), the Internal Revenue Service (IRS) Criminal Investigation (CI), Office of Inspector General (OIG) Social Security Administration (SSA), and Tigard Police Department (TPD). I was present at the meeting and spoke with TPD Detective Gabe Stone who was also present at the meeting. TPD Detective Stone met with an elderly male victim (hereinafter referred to as "V1"), who is approximately 78 years old. V1 told TPD Detective Stone that he was contacted by Ronnie Stevens in approximately September of 2016. V1 was selling a commercial trailer outside of his business in Newberg, Oregon when he was contacted



by Stevens. Stevens told V1 that he could help sell the commercial trailer for him. During the conversation, Stevens told V1 about an investment opportunity that involved the purchase of numerous classic cars and vans at a low price. According to Stevens, the classic cars and vans belonged to a man in Seattle, Washington who passed away. Stevens claimed the man's estate which included the classic cars and vans were left to the man's daughter as an inheritance. Stevens promised V1 that the vehicles could be purchased at a low price from Tammy Ward, the daughter of the deceased man.

10. TPD Detective Stone advised that shortly after the September of 2016 meeting, V1 provided Stevens an initial cash investment to purchase the classic cars and vans from the estate with a promise that the vehicles would be purchased at a low price. From approximately September of 2016, until approximately May of 2018, V1 and his wife (hereinafter referred to as "V2"), who is approximately 74 years old, provided Stevens with approximately \$2,500,000.00 in cash in multiple cash payments. V1 and V2 have never received any classic cars and/or vans and have not had their money returned to them. V1 and V2 obtained money from their retirement accounts, savings, checking, and from personal loans in order to pay Stevens.

11. On August 31, 2018, I interviewed V1 and V2 with TPD Detective Stone present at TPD. V1 told me that he is the business owner of a company located in Newberg, Oregon. V1 was originally contacted by Stevens when Stevens approached him regarding a commercial semi-trailer for sale at V1's business. V1 was selling the commercial trailer for approximately \$50,000.00. V1 is unsure how Stevens came to look at the semi-trailer. Stevens never bought the trailer from him or helped him sell the trailer.

12. After V1 met Stevens, Stevens told V1 about a hold up with Tammy Ward's

father's estate. Stevens told V1 that the estate was located somewhere north of Seattle, Washington and had about 120 classic cars and vans associated with the estate. V1 likes classic cars. V1 stated that Stevens told him that the estate had "every model" of classic car from Corvettes to expensive classic ones. V1 was also told by Stevens that some of the cars associated with Ward's estate were also located in Cucamonga, California.

13. V1 explained that Stevens told him that in order to get the classic cars and vans freed from the estate and into V1's possession, Stevens needed to pay the person who held the estate. V1 was never shown the classic cars or vans in person or ever shown a photo of the vehicles. V1 agreed to pay Stevens in order to obtain the vehicles after the estate was freed up. V1 first paid Stevens approximately \$15,000.00 in cash and then an additional approximately \$25,000.00 two weeks after the first payment.

14. Stevens continued to solicit additional funds from V1 to release the alleged estate. In total, V1 has paid Stevens approximately \$2,500,000.00 over the last year and a half. V1 has never received anything. Stevens continues to ask V1 and V2 for more money. Stevens communicates frequently with V1 and V2 over the telephone. When V1 and V2 ask about the deal, Stevens tells them that it is coming or things are in process.

15. At Stevens' request, V1 has only paid Stevens in cash. Also, at Stevens' request, when Stevens and V1 meet, it is in person and typically at the Elmer's restaurant in Tigard, Oregon or at an Elmer's restaurant off of Interstate 205 or in a parking lot.

16. At the time of the August interview with V1 and V2, Stevens had recently asked for an additional \$267,000.00. When Stevens asked for an additional \$267,000.00, Stevens told V1 that Sam Last Name Unknown (LNU) and Mike LNU were helping Stevens get the funds in

order to get the classic cars and vans to V1. Stevens wanted V1 and V2 to meet with Sam LNU in order to get him more money. Stevens told V1 that Sam LNU is his friend and lives in Eugene, Oregon. V1 and V2 are not comfortable with meeting Sam LNU.

17. V1 and V2 believe that Stevens is trying to get into their house and live there. Stevens have told the V1 and V2 that he has health issues and has nowhere to sleep.

18. V1 and V2 will return Stevens' telephone calls when they miss it. When the V1 and V2 return Stevens' telephone calls, the telephone calls always goes into Stevens' voicemail. Stevens then calls them back. V2 stated that Stevens seems to always have his telephone off. Stevens will ask questions of V1 and V2 as follows: Who's at their house, what is going on at their house, where are you going?

19. The investigation revealed that Stevens is not employed. Stevens told V1 that he is not employed but told V1 that he sells cars. V1 recalled that Stevens had a little red beat-up van and a white or tan suburban when they would meet each other at Elmer's restaurant. I have spoken to a Special Agent with OIG-SSA who informed me that Ronnie Stevens, Tim Ephrem, or Tina Ephrem are not believed to be employed and are not receiving any benefits from the Social Security Administration.

20. V1 has borrowed money from family, friends and the bank in order to provide Stevens the money. V1 and V2 also tapped into both of their accounts at Charles Schwab. Approximately \$800,000.00 was withdrawn from a personal account along with approximately \$360,000.00 from V1's Roth IRA and approximately \$50,000.00 from V2's Roth IRA. V1 and V2 have also cashed in approximately \$26,000.00 of gold and silver and provided the cash to Stevens. V1 and V2 also provided Stevens approximately \$30,000.00 in collectible bills in the

denomination of \$20s, \$50s, and \$100s. V1 took out a loan from the bank for approximately \$200,000.00 and cashed out approximately \$150,000.00 to give to Stevens. V1 also borrowed against his 401K and loaned himself approximately \$150,000.00 to \$200,000.00 in total to give to Stevens. V1 has also taken approximately \$80,000.00 against his business, which also went to Stevens. V1 stated that some of his company's fortunes got divided up when he became involved with Stevens.

21. V1 spoke on the telephone to Tammy Ward one time. V2 recalled that she spoke to Ward approximately three times on the telephone. V2 has asked Ward to meet in person but Ward has always denied to meet in person for some excuse. V1 stated that there were a couple of occasions when he spoke to Stevens over the telephone and Stevens was together with Ward. Stevens would put Ward on his telephone.

#### **Background – Ronnie Stevens**

22. A driver motor vehicle (DMV) records check of Ronnie Stevens shows that Stevens' date of birth is July 11, 1969, his social security number is 535-78-3850, height 5'6", weight 235 pounds, and eyes green. Stevens possesses a State of Washington identification card license number "STEVE\*316MJ" and address 5601 6<sup>th</sup> Avenue, Tacoma, Washington 98406, which was issued on November 26, 2014.

23. A criminal records check of Ronnie Stevens shows that Stevens is associated with FBI Number 672647AC1 and Washington State Identification (SID) WA14809772. The criminal records check shows that Stevens has used the following aliases which all possess the same date of birth of April 25, 1967: Tim J. Ephrem, Ron Stevens, Ron Stephens, and Ron Steves.



24. A DMV records check of Tim J. Ephrem shows that Ephrem's date of birth is April 25, 1967, his social security number is 542-59-7080, height 5'6", weight 260, and eyes blue. Tim Ephrem possesses a State of Washington driver's license number "EPHERTJ334J5" with address 4720 South Thompson, Tacoma, Washington 98408, which was issued on January 16, 2002.

25. I compared both Washington DMV photos of Stevens and Tim Ephrem. Both photos appear to be of the same male individual except Stevens' photo taken in 2014 showed Stevens as bald.

26. An open source database records check shows that Stevens' personally identifiable information (PII) is his true identity. It is believed that Tim Ephrem's PII belongs to another individual.

#### **Background – Tina Ephrem**

27. A DMV records check of Tina Ephrem shows that her date of birth is May 25, 1975, social security number 540-15-3767, height 5'1", and weight 115 pounds. Tina Ephrem possesses an Oregon identification card license number 5722396 and address 10358 SE Ellis Street, Portland, Oregon 97266, which was issued on December 20, 2012.

28. A criminal records check shows that Tina Ephrem is associated with FBI Number 750267KD2 and Oregon SID OR18800883. The criminal records check shows that Tina Ephrem has used the alias: Lisa Ann Peterson.

29. A DMV records check for Lisa Ann Peterson shows that Peterson's date of birth is July 21, 1973, her social security number is 534-88-9251, height 5'1", and weight 120 pounds. Peterson possesses a State of Oregon driver's license number 6752599 and address 13406 SE

Division Street, Apartment 14, Portland, Oregon 97236, which was issued on April 15, 2006.

30. I compared both Oregon DMV photos of Tina Ephrem and Peterson. Both photos appear to be of the same female individual. An open source database records check shows that Peterson's Oregon DMV license with the address 13406 SE Division Street, Apartment 14, Portland, Oregon 97236, was also associated to a previous address held by Tina Ephrem.

31. Based upon the investigation, it believed that Stevens and Tina Ephrem have presented as husband and wife since at least 2002 and are believed to also have a daughter. Stevens and Tina Ephrem are also associated to with the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086. It is believed that Stevens and Tina Ephrem live together at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086, based upon physical surveillance conducted by the FBI during summer and fall of 2018.

**Prior Fraudulent Conduct – Pierce County 2002 Fraud Scheme**

32. According to Pierce County Sheriff's reports for Incident No. 0310080450, in July 2002, victim R.S. met a woman by the name of "Lisa Stevens" (believed to be Tina Ephrem) through a personal ad in a local newspaper. Lisa Stevens asked R.S. for \$20,000, claiming she needed the funds for cancer treatment. R.S. sought the help of his son, K.S., and K.S. provided the funds to Lisa Stevens in cash.

33. After providing the cash to Lisa Stevens, she stated that her relative "Ted White" (later identified as Ronnie Stevens) needed help getting his family inheritance out of probate in Arizona. Lisa Stevens claimed that Ted White stood to inherit an estate from his deceased father, but could only claim the estate if Ted White fronted the funds for the taxes on the estate.

According to reports, Ted White steadily increased the alleged value of the estate, from \$740,000 to \$7,000,000. At each increase, and each request for additional cash, Ted White promised a greater return payment to R.S and K.S. The victims raised cash through credit card advances and annuities. Between December 2002 and February 2003, R.S and K.S. gave \$128,000 in cash to Lisa Stevens and Ted White during approximately 7 separate meetings. The victims reported that Lisa Stevens and Ted White requested cash because they did not have bank accounts to cash checks. Eventually, Ted called the victims directly with requests for additional cash. Ted White typically asked the victims to meet him at an Elmer's restaurant or at a store parking lot to exchange the cash.

34. On June 8, 2005, the Superior Court of Washington for Pierce sentenced Ronnie Stevens to 30 days jail for a felony theft conviction related to this fraud scheme (Pierce County Case number 031018696).

#### **Prior Criminal Conduct – Pierce County 2004 Fraud Scheme**

35. On August 31, 2005, victim C.F. filed a Complaint for Money Owed against defendants Tim Ephrem (aka Ronnie Stevens) and Tina Ephrem, identified in the complaint as husband and wife. According to the complaint allegations, Tim Ephrem befriended victim C.F. and solicited C.F. for loans in 2004 and 2005. In January 2005, Tim Ephrem asked C.F. for a \$39,000 loan. Tim Ephrem represented that he intended to use the loan to acquire motor homes and trucks, and that C.F. would receive short-term repayment or the interest in the purported motor home. On April 26, 2006, C.F.'s attorney deposed Tina Ephrem. In that deposition, Tina Ephrem claimed that neither she nor Tim Ephrem could read anything other than numbers.

#### **Prior Criminal Conduct – King County 2005 – 2007 Fraud Scheme**

36. Ronnie Stevens, his defense attorney, and a Senior Deputy Prosecuting Attorney signed and filed a Stipulation of Facts and Conclusions of Law Supporting an Exceptional Sentence dated July 9, 2012. In that Stipulation, Stevens admits that he befriended victim S.B. in 2005 and told S.B. that his deceased father left an estate worth \$500,000,000 and that Stevens would inherit the estate but needed money to pay lawyers and taxes. Stevens asked S.B. to loan him funds and promised S.B. one third of the estate assets in return. Between August 2005 and November 2005, S.B. provided Stevens \$2,362,680 in cash in 24 separate transactions. When S.B. ran out of funds, Stevens pressured S.B. to seek funds from friends or family, with the continued false promise of return. S.B.'s friend provided Stevens \$171,000 based on Stevens' representation that he would pay back three times the original investment within a month once the estate closed. In fact, Stevens' father did not leave any inheritance and had died in 1990. Stevens repaid none of the funds as promised.

37. On July 9, 2012, Stevens pleaded guilty to one count of theft in the first degree for fraud crimes against a single victim spanning August 2005 – November 2007, and one count of theft in the first degree for fraud crimes against another victim in August of 2006. On July 27, 2012, the Superior Court of Washington for King County sentenced Ronnie Stevens (aka Tim Ephrem) to 48 months incarceration for his role in two related fraud schemes. (Case No. 11-1-01457-2 KNT). The court ordered Stevens to pay restitution to the victims in the amount of \$2,437,611.91.

38. On August 16, 2018, the Superior Court of Washington for King County issued a bench warrant for Stevens for failure to appear for a sentence modification hearing. The court summoned Stevens to appear at hearing for his failure to make required payments toward his

court ordered restitution in Case No. 11-1-01457-2 KNT.

39. On December 3, 2018, Stevens was arrested by the Clark County Sheriff's Office for the outstanding bench warrant issued out of King County. Stevens was located at the Ilani Casino located in Ridgefield, Washington. Stevens was released by King County, Washington court on approximately December 10, 2018.

40. On December 11, 2018, I spoke with TPD Detective Stone who informed me that he spoke with V1 and V2 who told him that Stevens had not contacted V1 and V2 for approximately a week. V1 and V2 were not made aware of Stevens' arrest. Following Stevens release from police custody, Stevens telephonically contacted V1 and V2. When Stevens called V1 and V2 following his release from custody, Stevens did not tell V1 and V2 that he had been in police custody but instead that he had been out of touch with them because he received a concussion after falling and was now in a wheelchair.

**Prior Criminal Conduct – Multnomah County 2010 – Fraud Scheme**

41. According to Multnomah County Sheriff's Office reports in case number 10-405142, in 2009, "Tina Johnson" (later identified as Tina Ephrem) approached R.H. in a Fred Meyer. At the time, R.H. was in his late 70s and recently widowed. R.H. reported that Tina Johnson befriended him and gained his trust. By 2010, Tina Johnson regularly called R.H. at least three to four times a day. Tina Johnson reported that she lived with her brother "Tom" (later identified as Ronnie Stevens/Tim Ephrem). Tom made promises to meet R.H. in person, but never did. The two only spoke on the phone. R.H. regularly met Tina Johnson in public at restaurants or for coffee.

42. In approximately April 2010, Tina Ephrem told R.H. that she and her brother Tom



were to receive a \$20 million inheritance from a deceased uncle. Tina Johnson and Tom initially explained to R.H. that a \$6,000 lien prevented the release of the property and inheritance owed to Tina Johnson and Tom. Tina Johnson asked R.H. for help with funds to release the inheritance from the estate. In return, Tina Johnson promised R.H. a portion of the estate. After R.H. agreed to provide Tina with funds, Tina Johnson continued to report that attorneys applied additional liens to the estate and she needed more funds to release the estate. When R.H. ran short on funds, he introduced Tina Johnson to his friend K.P., also in his late 70s. Tina Johnson relayed the same story to K.P. K.P. also provided money to Tina Johnson with the promise of return from the released estate. According to the investigation, the subscriber on the mobile number Tina Johnson used to call R.H. was Tim Ephrem. On August 30, 2011, a Multnomah County judge sentenced Tina Ephrem to a reduced 15 months in prison after she provided the district attorney with two checks totaling \$180,800 for restitution to her two victims (Multnomah County case number 101234938).

43. In 2012, R.H. and K.P. jointly sought and received a civil limited judgment and money award against defendants Tina Ephrem and Ronnie Stevens, joint and several, in the total approximate amount of \$840,000 based on the victim's claims for relief for abuse of a vulnerable elderly person in connection with this fraud scheme.

#### **Financial Investigation – Victims' Funds**

44. The FBI performed a financial analysis on V1 and V2's bank account held with Columbia Bank. Columbia Bank is a federally-insured financial institution headquartered in Tacoma, Washington. V1 and V2 made financial transactions at Columbia Bank branches in the Portland metro area during the alleged fraud scheme conducted by Stevens.

45. At Stevens' request, V1 and V2 made approximately 50 cash withdrawals from Columbia Bank branches from approximately September of 2016, through March of 2018 from Columbia bank account number x7221. V1 sometimes made multiple cash withdrawals on a single day. For example, on approximately August 22, 2017, V1 withdrew \$75,000 in cash from three different Columbia Bank branches in the Portland metro area. Exhibit 1 shows examples of cash withdrawals made by V1 from various Columbia Bank branches.

Exhibit 1 Columbia Bank (x7221) Deposits and Withdrawals				
Date	Transaction Type	Deposit	Withdrawal	Notes
12/29/2017	deposit (Charles Schwab)	\$55,000		deposit (Charles Schwab)
12/29/2017	deposit (Charles Schwab)	\$59,000		deposit (Charles Schwab)
12/29/2017	Cash Withdrawal		\$70,000	cash withdrawal conducted by V1 at the Newberg branch;
12/29/2017	Cash Withdrawal		\$11,000	cash withdrawal conducted by V1 at the Tualatin-Sherwood branch
12/29/2017	Cash Withdrawal		\$40,000	cash withdrawal conducted by V1 at the King City branch;
12/29/2017	Cash Withdrawal		\$5,000	cash withdrawal conducted by V1 at the Tigard branch;
1/26/2018	Cash Withdrawal		\$50,000	cash withdrawal conducted by V1 at the Newberg branch;
1/26/2018	Cash Withdrawal		\$15,000	cash withdrawal conducted by V1 at the King City branch;
1/26/2018	Cash Withdrawal		\$20,000	cash withdrawal conducted by V1 at the Tualatin-Sherwood branch
1/26/2018	Cash Withdrawal		\$26,000	cash withdrawal conducted by V1 at the Lake Oswego branch

46. I spoke with a Columbia Bank representative who told me that sometimes its branches only carry a certain amount of cash on hand, which would explain why V1 made multiple cash withdrawals on a single day from different Columbia Bank branches.

47. TPD Detective Stone told me that once V1 made cash withdrawals, he immediately met with Stevens and provided Stevens the cash in person. V1 did not hold onto the cash for very long once it was withdrawn from his bank account. TPD Detective Stone also told me that Stevens only wanted cash from V1 and no checks, cashier checks or wire transfers.

48. V1 and V2 hold retirement accounts with Charles Schwab. Majority of the cash withdrawals provided to Stevens were funded by V1 and V2's Charles Schwab account.

49. From approximately May of 2017, through approximately March of 2018, V1 and V2 deposited approximately \$914,000.00 from their Charles Schwab accounts into their

Columbia Bank account. The deposited Charles Schwab checks were subsequently withdrawn in cash by V1 and V2 in order to pay Stevens.

50. Approximately 13 checks were issued to V1 and V2 from V1 and V2's Charles Schwab accounts and then deposited into V1 and V2's Columbia Bank account. The single largest check from Charles Schwab was \$193,000, which occurred on approximately August 9, 2017, and was deposited into V1 and V2's account at Columbia Bank. Exhibit 2 shows the checks issued to V1 and V2, which were deposited into their Columbia Bank account.

<b>Exhibit 2</b>				
<b>#</b>	<b>Date</b>	<b>Remitter</b>	<b>Payee</b>	<b>Amount</b>
1	5/17/2017	Charles Schwab	V1	\$ 68,000
2	6/16/2017	Charles Schwab	V1	\$ 90,000
3	7/5/2017	Charles Schwab	V1	\$ 35,000
4	7/18/2017	Charles Schwab	V1	\$ 37,000
5	8/9/2017	Charles Schwab	V1	\$ 193,000
6	8/21/2017	Charles Schwab	V1	\$ 110,000
7	9/7/2017	Charles Schwab	V1	\$ 60,000
8	11/13/2017	Charles Schwab	V1	\$ 80,000
9	12/7/2017	Charles Schwab	V1	\$ 17,000
10	12/7/2017	Charles Schwab	V2	\$ 50,000
11	12/29/2017	Charles Schwab	V1	\$ 55,000
12	12/29/2017	Charles Schwab	V1	\$ 59,000
13	3/9/2018	Charles Schwab	V1	\$ 60,000
				<b>\$ 914,000</b>

51. From approximately 2016, through 2018, the single largest cash withdrawal provided to Stevens was \$114,000.00 and the average cash withdrawal was approximately \$27,000.00. Exhibit 3 shows the total estimated cash withdrawals by V1 and V2 from approximately 2016, through 2018 only from their Columbia Bank account.



<b>Exhibit 3 (Columbia Bank x7221)</b>		
<b>Year</b>	<b></b>	<b>Cash Withdrawals</b>
2016	\$	6,600.00
2017	\$	1,095,300.00
2018	\$	302,000.00
<b>Grand Total</b>	<b>\$</b>	<b>1,403,900.00</b>

**Financial Investigation – Tina Ephrem Gambling**

52. The investigation revealed that Tina Ephrem was involved in gambling. An Oregonian article published on September 17, 2011, titled “Multnomah County’s Elder Fraud Unit Helps Expose ‘trusted friend’ as Con Artist” by Maxine Bernstein, highlighted Tina Ephrem’s conviction regarding her 2011 felony conviction. The article highlighted how Tina Ephrem defrauded two elderly victims in Multnomah County in an inheritance scheme. The article also highlighted how Tina Ephrem admitted to the judge at sentencing that she had a gambling problem.

53. The FBI obtained bank statements for Tina Ephrem’s Bank of America account. Tina Ephrem’s Bank of America account number is x1836. The Bank of America statements from February of 2018 showed Tina Ephrem made debit card purchases at the Bellagio casino in Las Vegas, Nevada.

54. The FBI obtained records from the Bellagio casino located in Las Vegas, Nevada for Tina Ephrem for the time period from approximately September of 2016, until present.

55. Exhibit 4 shows a summary of total cash used for cash buy for Tina Ephrem at the Bellagio casino from approximately December of 2016 until July of 2018.

Exhibit 4	
Tina Ephrem Las Vegas Spending Summary	
Bellagio	
Trip Dates	Total Cash Buy In
12/23/16-1/2/17	\$ 6,795.00
2/4/17-2/8/17	\$ 1,600.00
10/5/17-10/16/17	\$ 20,900.00
12/29/17-1/2/18	\$ 6,565.00
2/2/18-2/10/18	\$ 16,030.00
5/24/18-5/28/18	\$ 5,084.00
7/3/18-7/11/18	\$ 10,890.00
<b>Total:</b>	<b>\$ 67,864.00</b>

**Financial Investigation – Stevens/Tim Ephrem Gambling**

56. The FBI obtained records from the Wynn Las Vegas casino located in Las Vegas, Nevada regarding Stevens for the time period from approximately September of 2016, until present.

57. The Wynn Las Vegas casino made a copy of Stevens' State of Washington identification card when he visited the casino. The Wynn Las Vegas casino provided Stevens' players account number x3680, which was created on approximately December 25, 2016. Stevens also provided the casino social security number xxx-xx-3550. The investigation revealed that the social security number is believed to belong to a real individual in Texas not identified as Stevens.

58. The Wynn Las Vegas casino also provided information regarding Tim J. Ephrem's player's account number x8875, which was created in approximately April 28, 2007. The Wynn Las Vegas casino made a copy of Tim Ephrem's State of Washington driver's license. Tim Ephrem provided the casino social security number xxx-xx-3833. The investigation revealed that the social security number is believed to belong to a real individual in



Virginia not identified as Tim Ephrem.

59. The FBI obtained records from the Bellagio casino regarding Stevens for the time period from approximately September of 2016, until present.

60. The FBI analyzed records obtained from both the Wynn Las Vegas casino and Bellagio casino in Las Vegas, Nevada for casino records related to Ronnie Stevens. Exhibit 5 shows a summary of total cash used for cash buy in for Ronnie Stevens at the Wynn Las Vegas casino and Bellagio casinos from approximately December of 2016, until July of 2018.

<b>Exhibit 5</b>			
<b>Tim Ephrem/Ronnie Stevens Las Vegas Spending Summary</b>			
	<b>Bellagio</b>	<b>Wynn Las Vegas</b>	
<b>Trip Dates</b>	<b>Total Cash Buy In</b>	<b>Total Cash Buy In</b>	<b>Combined Cash Buy In</b>
12/23/16-1/2/17	\$ 2,200.00	\$ 600.00	\$ 2,800.00
2/4/17-2/8/17	\$ -	\$ 1,500.00	\$ 1,500.00
<b>*9/3/17-9/6/17</b>	\$ -	\$ 7,200.00	\$ 7,200.00
10/5/17-10/16/17	\$ 800.00	\$ -	\$ 800.00
12/29/17-1/2/18	\$ 2,080.00	\$ -	\$ 2,080.00
2/2/18-2/10/18	\$ 6,000.00	\$ 11,600.00	\$ 17,600.00
<b>*4/9/18-4/10/18</b>	\$ -	\$ 500.00	\$ 500.00
5/24/18-5/28/18	\$ 800.00	\$ 500.00	\$ 1,300.00
7/3/18-7/11/18	\$ 12,400.00		\$ 12,400.00
<b>Totals:</b>	<b>\$ 24,280.00</b>	<b>\$ 21,900.00</b>	<b>\$ 46,180.00</b>
<i>* Dates of travel to Vegas w/o Tina</i>			

61. The investigation also shows that Stevens and Tina Ephrem were in Las Vegas, Nevada on or about the same time as each other. It is alleged that Stevens played at the Wynn Las Vegas casino from approximately February 2, 2018, until February 8, 2018. On February 6, 2018, Stevens used his player's card x3680 at the Wynn Las Vegas casino and deposited \$10,500.00 in cash into his player's account number x3680. On February 5, 2018, Tina Ephrem deposited \$10,800.00 in cash into her player's account number x5425 at the Bellagio casino. It

does not appear that Stevens has a bank account.

### **Financial Investigation – Travel Records**

62. The FBI obtained records from Southwest Airlines that showed both Stevens and Tina Ephrem purchased airfare and traveled from Portland, Oregon to multiple destinations during the alleged scheme. Stevens and Tina Ephrem have visited Las Vegas, Nevada approximately seven times during the alleged scheme. Stevens and Tina Ephrem also traveled from Portland, Oregon to California and to Hawaii during the alleged scheme. The Southwest Airline records show that both Stevens and Tina Ephrem booked the same airfare and traveled together to and from the same destinations. Exhibit 6 shows only airline travel records of Stevens and Tina Ephrem.

<b>Exhibit 6</b>			
<b>Ronnie Stevens and Tina Ephrem Airline Travel</b>			
<b>Trip Dates</b>	<b>Destination</b>	<b>Traveler Name</b>	<b>Traveler Name</b>
12/23/16-1/2/17	Vegas	Ronnie Stevens	Tina Ephrem
2/4/17-2/8/17	Vegas	Ronnie Stevens	Tina Ephrem
4/22/17-4/28/17	Hawaii	Ronnie Stevens	Tina Ephrem
7/10/17-7/16/17	California	Ronnie Stevens	Tina Ephrem
10/5/17-10/16/17	Vegas	Ronnie Stevens	Tina Ephrem
12/29/17-1/2/18	Vegas	Ronnie Stevens	Tina Ephrem
2/2/18-2/10/18	Vegas	Ronnie Stevens	Tina Ephrem
5/3/18-5/7/18	Chicago	Ronnie Stevens	Tina Ephrem
5/24/18-5/28/18	Vegas	Ronnie Stevens	Tina Ephrem
7/3/18-7/11/18	Vegas	Ronnie Stevens	Tina Ephrem

The travel records from Southwest Airlines also confirm that Stevens and Tina Ephrem were in Las Vegas, Nevada from approximately February 2, 2018, until approximately February 10, 2018, which is consistent with financial records from the above-mentioned casinos.

### **Telephone Analysis**

63. The FBI obtained telephone records from T-Mobile of Stevens' cell phone number from the time period of September of 2016, until present. Stevens' cell phone number is (503) 489-3944. Stevens frequently called V1. From approximately September of 2016, until present approximately 5,336 outgoing calls were placed from Stevens' cell phone number to V1 and V2.

64. The investigation also showed that the cell phone records showed that Stevens' cell phone placed outgoing calls to telephone number (360) 558-8782, which was the next highest outgoing calls after V1 and V2. The telephone number (360) 558-8782 is believed to be associated with Tina Ephrem and the cell phone carrier is Sprint based upon records obtained by the FBI from Sprint.

65. Exhibit 7 shows the number of outgoing calls made from Stevens' cell phone number (503) 489-3944 by month and by year to V1 and V2.

///

///

///

///



<b>Exhibit 7</b>	
<b>2016</b>	
<b>Month</b>	<b>Number of Calls To V1</b>
September	1
October	4
November	81
December	117
<b>Total:</b>	<b>203</b>
<b>2017</b>	
<b>Month</b>	<b>Number of Calls To V1</b>
January	147
February	181
March	172
April	152
May	184
June	251
July	251
August	313
September	192
October	273
November	280
December	281
<b>Total:</b>	<b>2,677</b>
<b>2018</b>	
<b>Month</b>	<b>Number of Calls To V1 and V2</b>
January	372
February	320
March	542
April	467
May	665
June	90
<b>Total:</b>	<b>2,456</b>
<b>Grand Total:</b>	<b>5,336</b>

66. The investigation also showed outgoing calls made by Stevens to V1 from approximately February 2, 2018, through February 10, 2018, while Stevens and Tina Ephrem were Las Vegas, Nevada. Stevens called V1 approximately 69 times while Stevens was in Las Vegas, Nevada. The hours of the calls placed to V1 ranged between shortly after midnight and after 11:00 p.m. Exhibit 8 shows calls made by Stevens to V1 from approximately February 2, 2018, through February 10, 2018, when Stevens is believed to be in Las Vegas, Nevada.

**Exhibit 8\*****Stevens' Calls to V1 While in Las Vegas, NV**

<b>Date</b>	<b>Total (In Minutes)</b>	<b>Total Number Of Calls</b>
2/2/2018	7	2
2/3/2018	34	10
2/4/2018	18	5
2/5/2018	16	6
2/6/2018	35	13
2/7/2018	33	7
2/8/2018	40	12
2/9/2018	53	11
2/10/2018	6	3
<b>Total:</b>	<b>243</b>	<b>69</b>

\*NOTE: Call totals were adjusted for flight arrival and departures into Las Vegas and Portland and do not include calls less than 1 second in length

67. Further analysis of the telephone records of Stevens and the Bank of America account of Tina Ephrem showed that Tina Ephrem's Bank of America account x1836 made at least one payment to a T-Mobile account.

**Social Media**

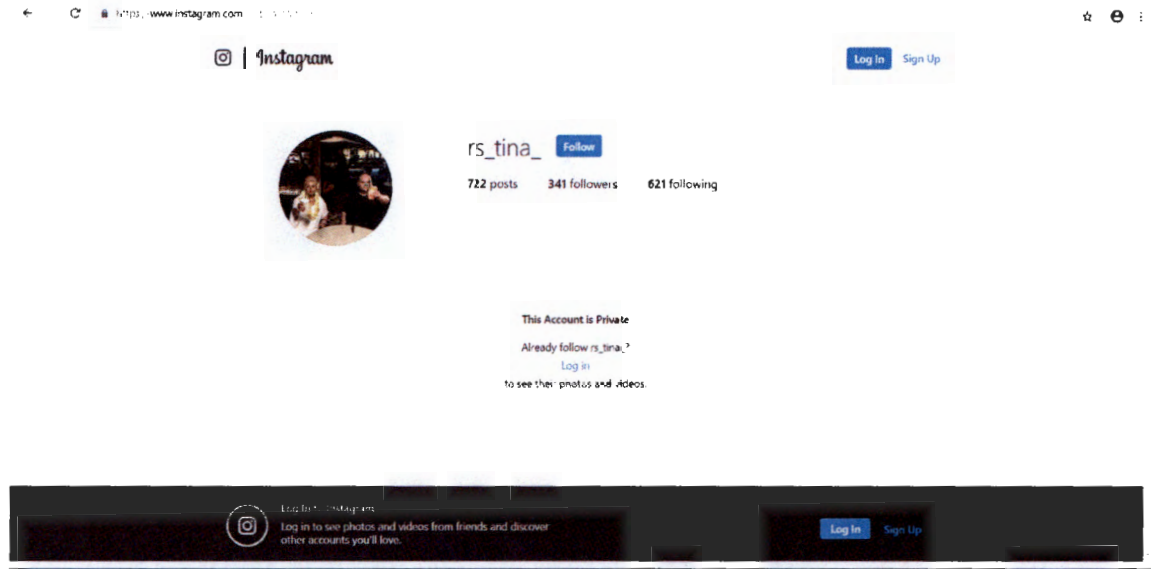
68. The investigation shows that Stevens and Tina Ephrem share a social media account with Instagram. The name of the account is believed to be "**rs\_tina\_**". Exhibit 9 below shows a snapshot taken on November 4, 2018 of the Instagram Account **rs\_tina\_**.

///

///

///





## Exhibit 9

The male and the female in the photo at the Instagram account resemble Stevens and Tina Ephrem. The Instagram Account is marked private and has 722 posts, 341 followers, and 621 following.

69. The investigation further shows that **rs\_tina\_** has posted comments on other Instagram accounts even though the Instagram account **rs\_tina\_** is a private account. The Instagram account “**peaches\_ephrem**” is an account believed to be associated to Peaches Ephrem. It is believed that Peaches Ephrem is related to Stevens and Tina Ephrem. In social media posts made by Peaches Ephrem, she refers to Tina Ephrem as her aunt and Stevens as her uncle.

70. Exhibit 10 shows the post made on May 25 by **peaches\_ephrem** who refers to “aunt Tina” in the photo. Tina is the female on the far right and Peaches Ephrem is the female located in the middle of the three individuals. In further review of the below photograph and its background from the post, the photograph appears to be taken in front of two large peacock

statues in an indoor setting. An open source search of the two large peacock statues resemble two large peacock statues and the indoor setting located at the Bellagio Conservatory located at the Bellagio casino in Las Vegas, Nevada. The date of the post by Peaches Ephrem also occurs during the time period where travel records show Stevens and Tina Ephrem in Las Vegas, Nevada.



Exhibit 10

71. Exhibit 11 shows a post made by Peaches Ephrem on July 12, regarding her “uncle rs.” Both individuals in the photograph resemble Stevens and Tina Ephrem. Peaches Ephrem references that “happy birthday” in her comments and **rs\_tina\_** replies “Ty.” The post was made on July 12, and Stevens’ birthday is July 11 based upon his Washington DMV license card.



Exhibit 11

72. Additional social media post made by Peaches Ephrem dated May 13, show another photo Tina Ephrem believed to be posing at the Kentucky Derby. Exhibit 12 shows Tina Ephrem and the post made by Peaches Ephrem.

///

///

///





Exhibit 12

**Information provided by Instagram**

73. On October 10, 2018, an order pursuant to 2703(d) was signed by United States Magistrate Judge Honorable Jolie A. Russo, Misc. No. '18-MC-924', which is under seal was served on Instagram LLC for Instagram account **rs\_tina\_**.

74. On October 29, 2018, Instagram LLC provided results regarding the Instagram Account **rs\_tina\_**. I reviewed the results from Instagram LLC for account **rs\_tina\_**. The Instagram Account was created on approximately September 15, 2015 and the registered e-mail used on the Instagram Account is e-mail account "tinars1975@icloud.com." The results from Instagram also show that the account **rs\_tina\_** accessed multiple Internet Protocol (IP) addresses from approximately September of 2016, until October of 2018. For example from the time

period of July 10, 2017, through approximately July 16, 2017, the Instagram Account accessed IP addresses in Los Angeles, California and suburbs of southern California. This is consistent with the above-stated travel records of Stevens and Tina Ephrem.

75. Furthermore, the Instagram Account also accessed IP addresses in Las Vegas, Nevada from approximately December 29, 2017, through approximately January 2, 2018, and from approximately February 2, 2018, through approximately February 10, 2018. This is also consistent with the above-stated travel records of Stevens and Tina Ephrem.

76. The Instagram Account showed activity with Instagram Direct which allows the user to send messages to one or more individuals. The user can send the following things as messages on Instagram Direct: Texts, media such as photos or videos, and likes. The Instagram Account showed that **rs\_tina\_** were on dozens of threads where the Instagram Account either authored or was a recipient of specific threads of conversation. The Instagram Account appeared to be associated with texts and media type within the threads.

77. On December 21, 2018, a Search and Seizure Warrant issued by the United States District Court for the District of Oregon, Portland Division, signed by US Magistrate Judge Youlee Yim You, Case No. '18-MC-1099, was obtained and executed on Instagram for the Instagram account **rs\_tina\_** and is pending a return from Instagram.

#### **Stored Cash**

78. Open source public database checks show that Lizzie Stevens is the mother of Ronnie Stevens. Open source public database checks also show that Lizzie Steve Stevens is also the mother of Tammy Stevens.

79. On November 10, 2009, Lizzie Stevens filed a claim for cash stored in a safe



deposit box at a financial institution located in Vancouver, Washington, which was seized by the federal government (Case No. CV 09-5179-RBL). Lizzie Stevens stated under penalty of perjury the following:

“Like almost all Roma men of his generation, my husband did not trust institutions of the gentile community. Because of this distrust, he did not put cash in bank accounts. Instead, he hid it in various places in and around our house. This was common practice in our community.”

80. On October 10, 2010, Multnomah County Sheriff’s Office (MCSO) executed a search warrant on Tina Ephrem’s residence located 3345 NE 126<sup>th</sup> Avenue, Portland, Oregon 97230 in conjunction with an investigation of Tina Ephrem regarding a theft by deception case (Case No. 10-405142). During the search, law enforcement officers seized approximately \$18,500.00 in cash.

**11412 SE Quail Run Drive, Happy Valley, Oregon 97086**

81. Bank statements obtained from the Bank of America show statements addressed to Tina Ephrem located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086 as of August of 2018. Records obtained from PGE show that Tina Ephrem is the current customer at the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086 as of November 2018. Furthermore, open source public database checks show that Stevens and Tina Ephrem are associated with the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086.

82. Open source public database checks shows that the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086 is owned by another owner. An Internet search

conducted on January 2, 2019, showed that the home was listed as a rental at “www.hotpads.com” and was taken off of the market on approximately September 28, 2017. The rental listed showed that the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086 is a 4 bedroom, two and a half bath three car garage residence that is approximately 3,000 square feet that was listed for approximately \$2,995.00 per month rental. The website also showed that the property is no longer available.

83. According to FBI physical surveillance conducted on October 30, 2018, individuals who resemble Stevens and Tina Ephrem departed in a red Dodge Caravan bearing Oregon license plate 179ETH from the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086. A records database check showed that the vehicle was a 2010 Dodge Caravan registered to Blake Michael Ristick of Portland, Oregon.

84. An Internet search showed that Ristick has an Instagram account, “**blakeristick**”. An Instagram post at **blakeristick** posted on October 6, 2018, contains a post and a video. The post referenced the following: “Birthday shout out to my cousin ‘@bxxxx\_bxxx\_2018’...” The post referenced his girl cousin who appears to be the daughter of Stevens. The Instagram post has a video of an individual who also resembles Stevens. The video shows Stevens in the passenger seat of a light green convertible Volkswagen Beetle being driving by a female.

85. According to FBI physical surveillance conducted on November 5, 2018, an individual who resembles Stevens departed in a red Dodge Caravan from the residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086.

86. According to FBI physical surveillance conducted on November 27, 2018, individuals who resemble Stevens and Tina Ephrem departed in a red Dodge Caravan from the

residence located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086.

87. Following his appearance in the Superior Court of King County on December 10, 2018, Stevens provided the court with an updated mailing address of 1155 SE 82<sup>nd</sup> Avenue, Portland, Oregon, but not the Quail Run Drive address. Open source research of the address shows that the address on 82<sup>nd</sup> is associated with Emerald Motors. A business name search conducted with the Oregon Secretary of State showed that Emerald Motors is an active business entity registered with the State of Oregon, since approximately March 17, 2016.

88. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

89. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know that Stevens and Tina Ephrem use cell phones to communicate with each other, and Stevens communicates with V1 and V2 using a cell phone. Furthermore, I know that the Instagram account **rs\_tina\_** is utilized by Stevens, Tina Ephrem or both, which requires the use of a computer and/or digital device. I know:

- a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years

at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data.

Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

90. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the



purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

- a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the

digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

- c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in

advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a digital device to commit a crime such as wire fraud, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

91. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

- a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore,



searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

92. In my training and experience, it is likely that the Premises will contain at least one Apple brand device, such as an iPhone or iPad, because in the records returned by Instagram for the Instagram account “**rs\_tina\_**”, Instagram provided the registered e-mail address “**tinars1975@icloud.com.**”

93. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

94. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a

more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

95. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

96. The passcode or password that would unlock the Apple device found during the search of the Premises is not known to law enforcement. Thus, it will likely be necessary to press the fingers of the users of the Apple device found during the search of the Premises to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the users is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

97. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the

device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the Premises to press their fingers against the Touch ID sensor of the locked Apple device found during the search of the Premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID. Based on these facts and my training and experience, it is likely that Ronnie Stevens, also known as Tim Ephrem, Tim J. Ephrem, Ron Steves, Ron Stevens, Ron Stephens, and Tina Ephrem, also known as Lisa Peterson is one user/are users of the device(s) and thus that their fingerprints are among those that are able to unlock the device via Touch ID.

98. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the Premises as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

99. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of the above-named individuals found at the Premises to the Touch ID sensor

of the device(s), such as an iPhone or an iPad, found at the Premises for the purpose of attempting to unlock the device(s) via Touch ID in order to search the contents as authorized by this warrant.)

#### **Nature of Investigation**

100. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

101. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

102. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data



falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

103. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

104. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

105. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

106. The government has made the following prior efforts in other judicial fora to obtain evidence sought under the warrant: Federal Grand Jury subpoenas, Title 18 U.S.C. § 2703(d) order, a search and seizure warrant for the Instagram account rs\_tina\_.

#### **Filter Team**

107. The government will utilize a "filter" agent to mitigate the review of privileged communications, if necessary. A special agent not assigned to investigate this case will be

designated as the "filter" agent and will utilize software to search the records for potential non-relevant and privileged communications, i.e. attorney-client communications. The "filter" agent will separate the identified privileged communications and then provide the remaining non-privileged communications available for search by the case agent.

### **Conclusion**

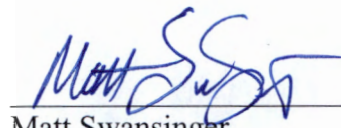
108. Based on the foregoing, I have probable cause to believe, and I do believe, that Ronnie Stevens and Tina Ephrem conspired to commit wire fraud in violation of Title 18, United States Code, § 1349, Conspiracy, and Title 18, United States Code §1343, wire fraud, and that evidence of that/those offense(s), as more fully described in Attachment B hereto, are presently located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086, which is described above and in Attachment A hereto. I therefore request that the Court issue a warrant authorizing a search of the Premises described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

109. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Donna Brecker Maddux and AUSA Maddux advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

### **Request for Sealing**

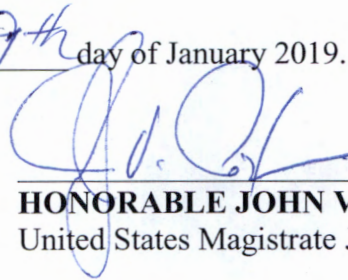
110. I further request that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these

documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may endanger the life or physical safety of an individual, cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.



Matt Swansinger  
Special Agent, FBI – Portland Division

Subscribed and sworn to before me this 9<sup>th</sup> day of January 2019.



**HONORABLE JOHN V. ACOSTA**  
United States Magistrate Judge

## **ATTACHMENT A**

### **Place to Be Searched**

Based on the information contained in this affidavit, I am requesting a warrant to search the following location:

The property located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086; is described as a two story, brown colored home, with dark colored shingles, and a three car garage. The property faces north. The address numbers “11412” are dark colored numbers embedded on the trim above the two car garage door to the left and near an outside porch light attached to the residence. The home is located on the corner of SE Quail Run Drive and SE Hillside Drive.



**ATTACHMENT B****Items to Be Seized**

The items to be searched for, seized, and examined, are those items on the premises located at 11412 SE Quail Run Drive, Happy Valley, Oregon 97086, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of United States Code, Section 1349, Conspiracy, and Title 18 United States Code, Section 1343, Wire Fraud. The items to be seized cover the period of September 01, 2016, through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined associated with Ronnie Stevens, also known as Tim Ephrem, Tim J. Ephrem, Ron Steves, Ron Stevens, Ron Stephens, and Tina Ephrem, also known as Lisa Peterson are as follows:
  - a. Cash, cash in collectible bills in denominations of \$20s, \$50s, and \$100s;
  - b. Financial records including bank statements, cancelled checks, deposit records, check stubs, payment ledgers, checkbook registers, deposit slips, loans, documentation of assets and liabilities, general ledgers, general journals, cash, cash receipts, cash disbursement journals, wire transfers, cashier checks, money orders, and records of bills relating to the receipt of currency or other forms of payment;
  - c. Records of credit card and automatic teller machine activity, including credit and/or debit cards, pre-paid debit cards, and automatic teller machine records;
  - d. Estate and property related documentation regarding the Tammy Ward estate,

also referred to as the Ward estate;

- e. Records, receipts, statements, and/or transaction history for casino related entities, gambling winnings, players' cards/accounts, and/or correspondence;
- f. Records, information or documents that reflect the use of mailing addresses such as Post Office Boxes;
- g. Photos, passports, photo identification and other identification for aliases or nominees use by Ronnie Stevens, also known as Tim Ephrem, Tim J. Ephrem, Ron Steves, Ron Stevens, Ron Stephens, and Tina Ephrem, also known as Lisa Peterson;
- h. Correspondence to and from Ronnie Stevens, also known as Tim Ephrem, Tim J. Ephrem, Ron Steves, Ron Stevens, Ron Stephens, and Tina Ephrem, also known as Lisa Peterson, including letters, cards, other written correspondence, facsimiles, e-mails, printed e-mails, taped messages such as answering machine messages, and videos that are related to Tammy Ward, V1/A.F. and V2/S.F. (The names of the initials are known to the government);
- i. Payroll and payroll tax records including timecards, timesheets, handwritten hour summaries, payroll sheets/journals, payroll check registers, canceled payroll checks, paycheck stubs, Forms W-2, Forms W-4, Forms 941, Forms 940, and Forms 1099;
- j. Business licenses, stock certificates, logs of stock purchases and redemptions, joint venture agreements, teaming agreements, subcontract agreements, lease agreements, employee sharing agreements;

- k. Calendar books, log books, appointment books, and telephone number listings;
- l. Documents reflecting travel expenditures to include copies of travel tickets, hotel bills, gas receipts, and copies of payment items comprising evidence of expenditures and liabilities;
- m. Notes payable and receivable, IOUs, and other recordation of debts comprising evidence of loans and expenses;
- n. Papers, records, documents, files, notes, memos, mail, or other materials representing residency, ownership, occupancy, dominion, or control of the premises referenced above and described in Attachment A;
- o. Records and/or keys showing actual or constructive possession of safe deposit boxes, safes, storage units, and any other type of storage areas, including passwords and/or access codes for access during the searches;
- p. Evidence of ownership or control of assets purchased since September of 2016.

2. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term

“storage medium” includes any physical object upon which computer data can be recorded.

Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter

“Computer”):

- a. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- b. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user;
- c. Evidence indicating the Computer user’s state of mind as it relates to the crime under investigation;
- d. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence;
- e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;
- f. Evidence of the times the Computer was used;
- i. Passwords, encryption keys, and other access devices that may be



- necessary to access the Computer;
  - j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;
  - k. Records of or information about Internet Protocol addresses used by the Computer;
  - l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
  - m. Contextual information necessary to understand the evidence described in this attachment;
  - n. Routers, modems, and network equipment used to connect computers to the Internet.
4. During the execution of the search of the Premises described in Attachment A, law enforcement personnel are authorized to press the fingers, including thumbs, of (name the individuals) found at the Premises to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the Premises for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

#### **Search Procedure**

5. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any

computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

6. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.
7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.
8. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the

computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

9. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.
10. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.